Chae$ 4: New Chaes Malware Variant Targeting Financial and Logistics Customers

blog.morphisec.com/chaes4-new-chaes-malware-variant-targeting-financial-and-logistics-customers

Hido Cohen & Arnold Osipov

Posted by Hido Cohen & Arnold Osipov on September 5, 2023
Find me on:
LinkedIn

- Tweet
-

MORPHISEC
THREAT PROFILE
CHAE$ 4 MALWARE
Morphisec Uncovers a New Chaes Malware Variant Targeting Financial and Logistics Industries

Exclusive: Morphisec Threat Labs identified Chae$ 4, an advanced and previously unknown variant of the Chaes malware. Read this post for an abstract of the findings.

Download the full Cha$ 4 technical analysis containing exclusive details of the threat.

Introduction - Chae$ 4

As the world of cyber threats evolves at an astonishing pace, staying ahead of these digital dangers becomes increasingly critical for businesses. In January 2023, Morphisec identified an alarming trend where numerous clients, primarily within the logistics and financial sectors, were under the onslaught of a new and advanced variant of Chaes malware. The sophistication of the threat was observed to increase over multiple iterations from April to June 2023.

Thanks to Morphisec's cutting-edge AMTD (Automatic Moving Target Defense) technology, many of these attacks were thwarted before causing significant damage.

This isn't just any ordinary Chaes variant. It has undergone major overhauls: from being rewritten entirely in Python, which resulted in lower detection rates by traditional defense systems, to a comprehensive redesign and an enhanced communication protocol. Additionally, it now boasts a suite of new modules that further its malicious capabilities.

The targets of this malware are not random. It has a specific focus on customers of prominent platforms and banks such as Mercado Libre, Mercado Pago, WhatsApp Web, Itau Bank, Caixa Bank, and even MetaMask. Furthermore, dozens of CMS (Content Management) services haven't been spared either, including WordPress, Joomla, Drupal and Magento. It's important to note that the Chaes malware isn't entirely new to the cybersecurity landscape. Its first appearance dates back to November 2020, when researchers from Cybereason highlighted its operations primarily targeting e-commerce customers in Latin America.

The new Chaes variant has been named “Chae$ 4” (Chae$4) by Morphisec, as it is the 4th major variant, and due to a debug print in a core module saying "Chae$ 4".

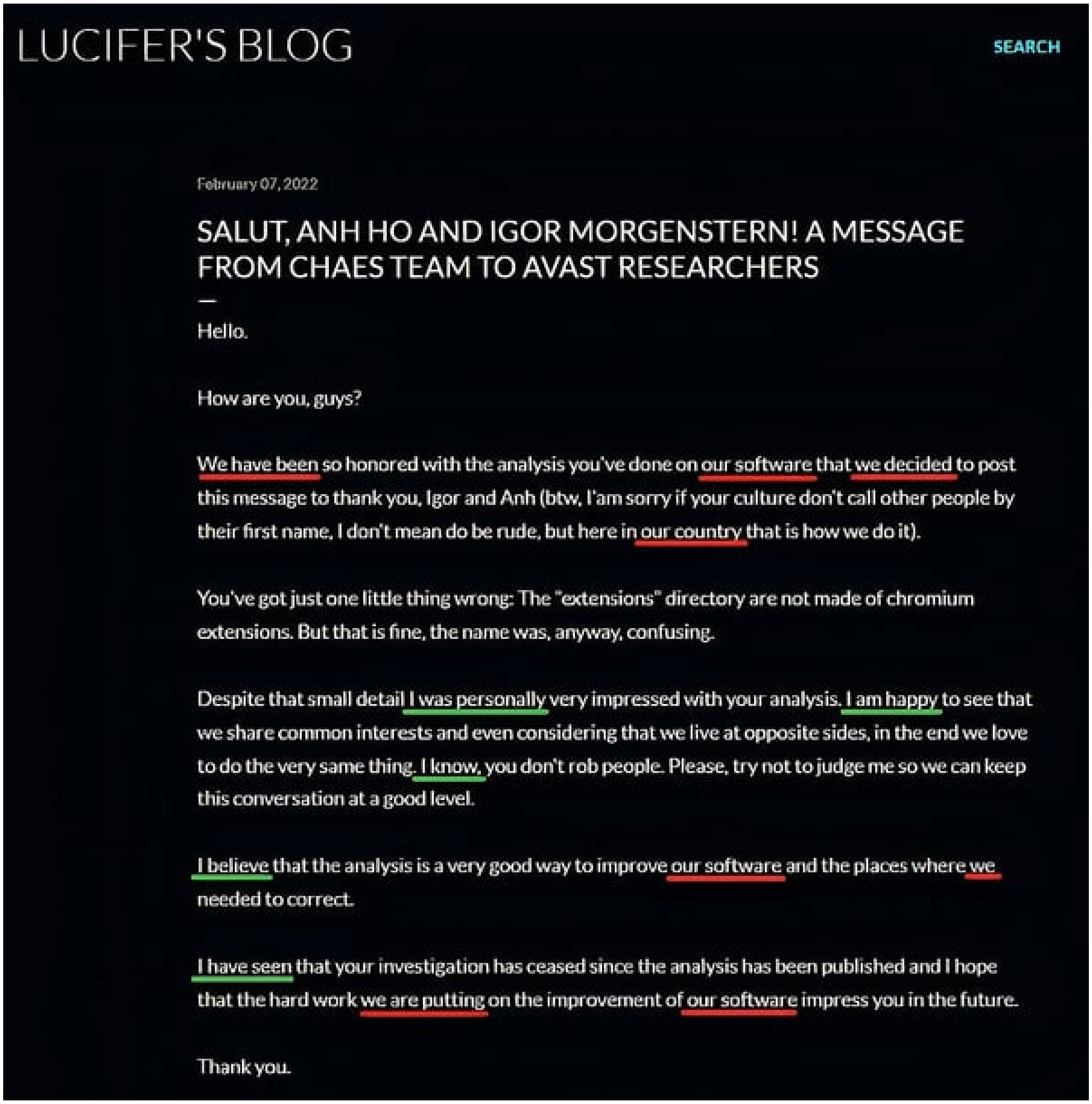
Chaes History & Overview

In **November 2020**, Cybereason released its initial research on the Chaes malware. The report highlighted that the malware had been active since at least mid-2020, predominantly targeting e-commerce customers in Latin America, especially Brazil.

Primarily, the malware targeted MercadoLibre users and was characterized by its multi-staged infection process, ability to steal sensitive and financial data related to MercadoLibre, and its utilization of multiple programming languages and LOLbins.

By **January 2022**, Avast published a subsequent study, indicating a surge in Chaes' activity during Q4 2021. Avast delved deeply into the different components of the malware, shedding light on its latest updates: a refined infection chain, enhanced communication with the C2, newly integrated modules (which they termed "extensions"), and granular details regarding each infection stage and module.

A few weeks later, in **February 2022**, the threat actor released a response to Avast's research as depicted in the image below:


LUCIFER'S BLOG

February 07, 2022

SALUT, ANH HO AND IGOR MORGENSTERN! A MESSAGE FROM CHAES TEAM TO AVAST RESEARCHERS

—

Hello.

How are you, guys?

We have been so honored with the analysis you've done on our software that we decided to post this message to thank you, Igor and Anh (btw, I'am sorry if your culture don't call other people by their first name, I don't mean do be rude, but here in our country that is how we do it).

You've got just one little thing wrong: The "extensions" directory are not made of chromium extensions. But that is fine, the name was, anyway, confusing.

Despite that small detail I was personally very impressed with your analysis. I am happy to see that we share common interests and even considering that we live at opposite sides, in the end we love to do the very same thing. I know, you don't rob people. Please, try not to judge me so we can keep this conversation at a good level.

I believe that the analysis is a very good way to improve our software and the places where we needed to correct.

I have seen that your investigation has ceased since the analysis has been published and I hope that the hard work we are putting on the improvement of our software impress you in the future.

Thank you.

Determining the nature of the threat actor—be it an individual or a group—proved elusive. Highlighted portions in red hint at the possibility of a group, while the green highlights reflect personal annotations. Given the ambiguity of the actor's identity, the designation "Lucifer" was chosen for this threat actor. This decision was influenced by the name of the blog and the identifier "lucifer6," used in encrypting communications with the C2 server.

Concluding the series of developments, **December 2022** marked another pivotal moment when the Tempest's research group, SideChannel, unveiled further insights, introducing the malware's adoption of WMI for system data collection.

Progressing to Version 4

These previously mentioned research publications encompass versions 1-3 of the Chaes malware. This latest iteration of Chaes unveils significant transformations and enhancements, and is labelled by Morphisec as version 4.

Significant changes include:

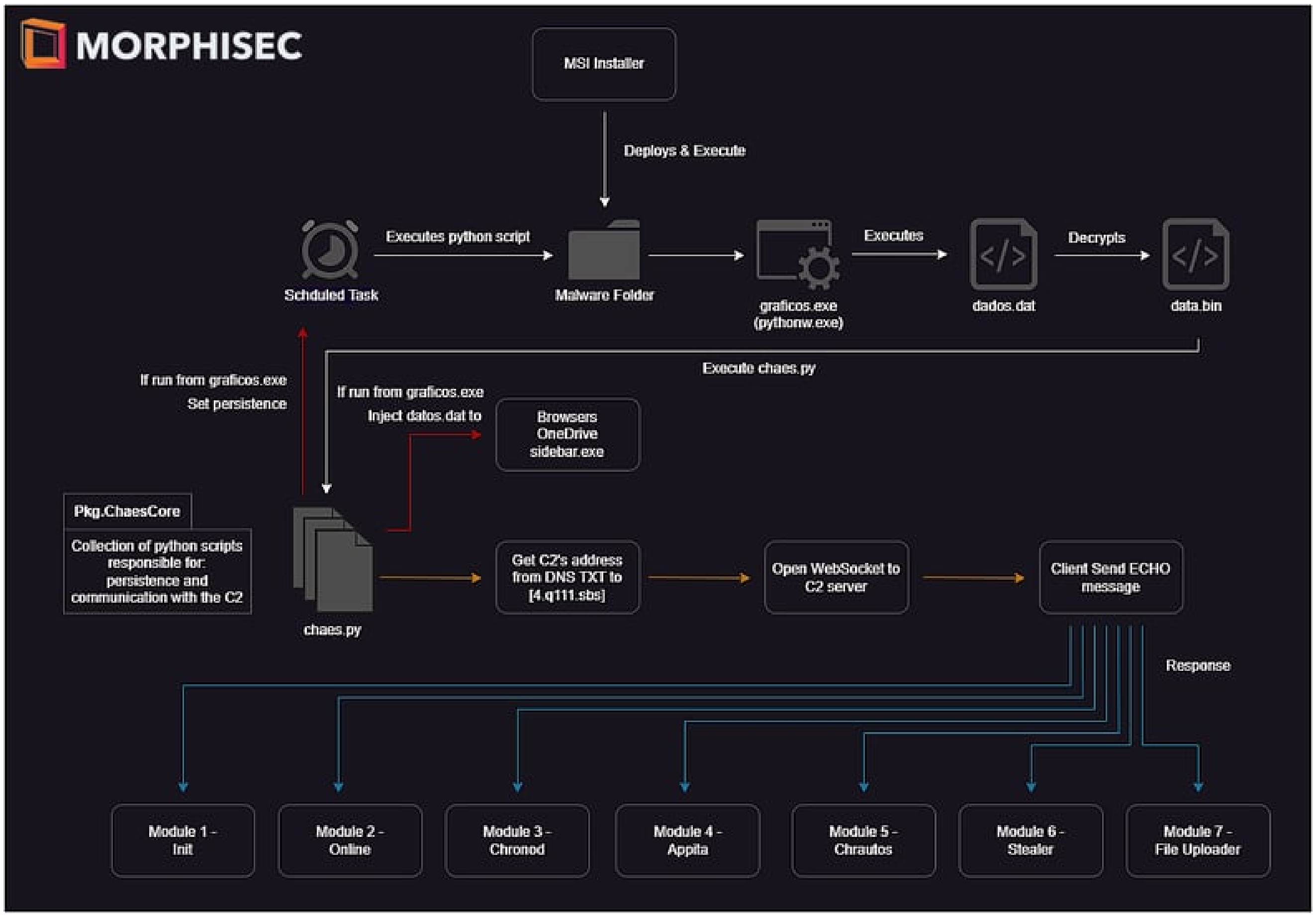
- Refined code architecture and improved modularity
- Added layers of encryption and increased stealth capabilities
- Predominant shift to Python, which undergoes decryption and dynamic in-memory execution
- Superseding Puppeteer with a bespoke approach to monitor and intercept Chromium browsers' activity
- An expanded catalog of services targeted for credential theft
- Adoption of WebSockets for primary communication between the modules and the C2 server
- Implementation of DGA for dynamic resolution of the C2 server's address
- Given the depth and breadth of content in this review, the analysis is structured to cater to a wide array of readers, ranging from SOC & CISOs to detection engineers, researchers, and security aficionados.

The analysis begins with an overview of the infection chain, which remains relatively consistent, followed by a succinct summary of each of the malware's modules. Subsequent sections will delve deeper into the specifics of each stage/module.

Since the malware employs recurring mechanisms across various stages/modules, we've designated a section titled "Additional Components." Here, readers can find intricate details about each mechanism cited throughout the post.

This structured approach ensures readers can either glean a rapid overview of the malware or immerse themselves in its intricate components.

Components



Note: Since there's no major updates in the delivery method from previous analysis and research notes (referenced earlier), this review will focus on recent developments. For those who aren't familiar with the infection method, please refer to the referenced research.

The infection starts by executing a malicious, almost undetected, MSI installer that usually pretends to be a JAVA JDE installer or Anti-Virus software installer. Execution of the malicious installer will cause the malware to deploy and download its required files inside a dedicated and hard-coded folder under the %Appdata%/<protuhuese_name> folder.

The folder contains Python libraries, Python executables with different names, encrypted files and Python scripts that will be used later. Next, the malware unpacks the core module, which we call ChaesCore — that is responsible for setting persistence using Schedule Task and migrating into targeted processes. After the initialization phase, ChaesCore starts its malicious activity and communicates with the C2 address in order to download and load the external modules into the infected system.

*Throughout this investigation, **seven** different modules were identified that can be updated independently without changing the core functionality:*

1. **Init module** - the first module sent by the attacker acts as an identification / new victim registration. It gathers an extensive amount of data on the infected system.
2. **Online module** - sends an ONLINE message back to the attacker. Acts like a beaconing

module to monitor which of the victims are still active.
3. **Chronod module** - a credential stealer and clipper. This module is responsible for intercepting browser activity to steal information from the user such as credentials sent on the login process, banking information when communicating with the bank's website, and has a clipping functionality that tries to steal BTC, ETH and PIX transfers.
4. **Appita module** - very similar to the Chronod module in structure and purpose but looks like it specifically targets the Itau bank's application (itauaplicativo.exe).
5. **Chrautos module** - an improved module based on Chronod and Appita modules. It provides better code architecture that has the capacities to expand the targets and tasks done by the module easily. The current version focuses on banking and WhatsApp data, however it's still under development.
6. **Stealer module** - responsible for stealing data from Chromium-based browsers. Stolen data includes login data, credit cards, cookies, and autofill.
7. **File upload module** - has the capability to search and upload files from the infected system to the C2 server. In the current version, the module uploads only data related to MetaMask's Chrome extension.
Most of the modules were already present in some form in previous versions, but this version provides a re-implementation for those with improved functionalities, different code base and unique techniques for achieving its goals.

Another thing to note is the threat actor’s keen interest in cryptocurrency, which is denoted by the usage of the clipper to steal BTC and ETH and the file upload module that steals MetaMask credentials and files.

Full technical analysis of Chae$ 4

The attached report dives deeper into each component of the framework. Starting from the MSI Installer, moving forward to the main component, the ChaesCore and finishing with the seven modules.

Finally, the different mechanisms used by the malware author for the general malware operation will be explored.

Download the Chae$ 4 full analysis to delve deeper into the mechanics of this evolved malware, its implications, and what businesses can do to safeguard themselves.

Or, hear directly from our team during our upcoming live, virtual event - Dancing With Lucifer: Behind the Scenes with the Analyst that Cracked Chae$ 4.

How Morphisec helps

Morphisec’s Automated Moving Target Detection (AMTD) uses a preventative approach to cybersecurity, using an ultra-lightweight agent to block unauthorized processes deterministically, rather than probabilistically. Protecting over 5,000 organizations and deployed at over nine million endpoints, Morphisec's AMTD technology prevents unauthorized code from executing, regardless of whether a recognizable signature or behavior pattern exists.

With the ability to proactively prevent unknown and evasive threats such as Chae$ 4, it is no wonder that Gartner described AMTD as "The future of cyber." Read the complimentary research report to learn more.